POHJOIS-KARJALAN AMMATTIKORKEAKOULU
Teknologiaosaamisen johtamisen koulutusohjelma
Ylempi ammattikorkeakoulututkinto

Markus Kuivalainen

VALMISTAUTUMINEN ISO/IEC 27001 STANDARDIN SERTIFIOINTIIN

Opinnäytetyö
Joulukuu 2011

POHJOIS-KARJALAN
AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Joulukuu 2011
Teknologiaosaamisen johtamisen
Koulutusohjelma
Karjalankatu 3
80200 JOENSUU
p. (013) 260 6700

Tekijä(t)
Markus Kuivalainen

Nimeke
Valmistautuminen ISO/IEC 27001 standardin sertifiointiin

Toimeksiantaja
Cygate Oy, Metsänneidonkuja 6, 02130 Espoo

Tiivistelmä

Tämän opinnäytetyön tarkoituksena on kuvata ISO/IEC 27001 -standardin vaatimukset organisaatioille. Opinnäytetyö käsittelee standardin eri osa-alueet sekä kuvaa ISO/IEC 27001 -standardin sertifiointiprosessin eri vaiheet kattavasti. Nämä osa-alueet muodostavat opinnäytetyön teoriaosuuden.

Opinnäytetyö on luonteeltaan kehitystehtävä. Kehitystehtävän kohteena on tietoliikenne- ja tietoturvajärjestelmien hallintaa ja valvontaa tarjoavan Cygate Oy:n valmistautuminen ISO/IEC 27001 -standardin sertifiointiin. Opinnäytetyön toinen osio kuvaa Cygaten kehitysprojektin vaiheet ja tulokset sekä jatkotoimenpiteet. Opinnäytetyön liite on salainen.

Kieli
suomi

Sivuja 50
Liitteet 1
Liitesivumäärä 24

Asiasanat
ISO/IEC 27001, tietoturvallisuus, hallintajärjestelmä

NORTH KARELIA
UNIVERSITY OF APPLIED SCIENCES

THESIS
December 2011
Degree Programme in Technology
Competence Management
Karjalankatu 3
80200 JOENSUU
tel. +358 (0)13 260 6700

Author (s)
Markus Kuivalainen

Title
Preparation for ISO/IEC 27001 standard certification

Commissioned by
Cygate, Metsänneidonkuja 6, 02130 Espoo

Abstract

This master's thesis describes the requirements of ISO/IEC 27001 standard in organizations. Thesis presents the demands of standard, and describes the certification process of ISO/IEC 27001 standard. These parts comprise the theory part of the thesis.

Thesis' nature is a development task. Target for the development is to prepare Cygate's organization for the ISO/IEC standard certification. The second part of this thesis describes the phases and the results of development project. Thesis also describes the next steps for Cygate to achieve certification and the conclusions of the project. The appendix of this thesis is classified as secret.

Language
Finnish

Pages 50
Appendices 1
Pages of Appendices 24

Keywords

ISO/IEC 27001, security, management system

SISÄLTÖ

LYHENTEET

DP	Decision Point, projektinaikainen päätöksentekopiste.
IEC	International Electrotechnical Commission, kansainvälinen sähköteknisen alan standardisointiorganisaatio.
IP	Internet Protocol, Internetin verkkokerroksen yhteyskäytäntö.
ISMS	Information Security Management System, tietoturvallisuuden hallintajärjestelmä.
ISO	International Organization for Standardization, kansainvälinen standardoimisorganisaatio.
ISO9001	Kansainvälinen standardi joka määrittelee laadunhallintajärjestelmien vaatimukset.
ISO14001	Kansainvälinen standardi ympäristön hallintajärjestelmälle.
SOA	Statement of Applicability, ISO 27001 standardin soveltamissuunnitelma.

1 JOHDANTO

Tietoturvallisuuden merkitys organisaatioissa on noussut entistä tärkeämpään rooliin kasvaneiden tietoturvauhkien takia. Uusia tietoturvauhkia kohdistuu organisaatioiden toimintaan jatkuvasti muuttuneiden toimintatapojen ja -ympäristöjen johdosta. Tänä päivänä useiden organisaatioiden päivittäinen toiminta on riippuvainen tietojärjestelmien toiminnasta.

Organisaation toiminnan riippuvuus tietojärjestelmien toiminnasta asettaa tietojärjestelmien ja tietoturvallisuuden hallinnan merkittäväksi asiaksi organisaatioiden sisäisen toiminnan ja toisaalta myös eri sidosryhmien välisen toiminnan suhteen. Tämän takia tietoturvallisuuden hallintaan on panostettava organisaatioissa riippumatta niiden koosta, tyypistä tai toiminta-alueesta. Tässä opinnäytetyössä kuvattava ISO/IEC 27001 tarjoaa kaiken tyyppisille organisaatioille hyvät ja kattavat menetelmät tietoturvallisuuden hallintaan.

2 OPINNÄYTETYÖN TAVOITTEET JA RAKENNE

Tämän opinnäytetyön tavoitteena on kuvata ISO/IEC 27001:2005 -standardin vaatimukset, ja kuvata tarvittavat toimenpiteet kehitysprojektin kautta Cygate Oy:n käytettävyyspalveluiden osalta valmistautuessa standardin sertifiointiin. Opinnäytetyö käy läpi ISO/IEC 27001:2005 -standardin vaatimukset ja nykytilan Cygaten käytettävyyspalveluiden osalta standardivaatimuksiin peilaten. Lisäksi opinnäytetyö kuvaa yrityksen valmistautumisen standardin sertifiointiin kehitysprojektin kautta.

Opinnäytetyö jakaantuu kahteen osaan: teoriaosuuteen ja kehitysprojektiin ja sen tuotoksiin. Teoriaosuus käy läpi ISO/IEC 27001 -standardin vaatimukset yksityiskohtaisesti sekä kuvaa standardin sertifiointiprosessin (kappaleet 1–4). Kehitysprojektiosuus ja johtopäätökset kuvaavat ISO/IEC 27001 -standardin

sertifiointiin valmistelevan projektin vaiheet Cygate Oy:ssä sekä projektin tuotokset johtopäätöksineen ja jatkotoimenpiteineen (kappaleet 5–7).

3 ISO/IEC 27001 -STANDARDI

ISO/IEC 27001 on kansainvälisten ISO- ja IEC- standardisointiorganisaatioiden luoma standardi tietoturvallisuuden hallinnalle organisaatioissa. Standardi on luotu malliksi organisaatioille tietoturvallisuuden hallintajärjestelmän (ISMS) kehittämiselle, toteuttamiselle, käyttämiselle, valvomiselle, katselmoinnille, ylläpitämiselle ja parantamiselle erityyppisissä organisaatioissa. Standardin avulla sekä sisäiset ja ulkoiset sidosryhmät voivat hyödyntää standardia arvioidessaan organisaation tietoturvallisuuden toteutumista sekä vaatimustenmukaisuutta. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Standardin käyttöönotto ja luominen ovat tyypillisesti organisaatioissa strateginen päätös. Standardin avulla organisaatio varmistaa ja osoittaa toiminnassaan, että se pyrkii toteuttamaan eri sidosryhmien kanssa toimiessaan tietojen luottamuksellisuuden, eheyden, käytettävyyden sekä kiistämättömyyden:

- *Luottamuksellisuus* tarkoittaa, että tieto on saatavilla ainoastaan sen käsittelyyn oikeutetuille tahoille.
- *Eheys* tarkoittaa tiedon ja tietojärjestelmien toiminnan virheettömyyden varmistamista.
- *Käytettävyys* tarkoittaa, että tiedot ovat aina tarvittaessa saatavilla.
- *Kiistämättömyys* tarkoittaa, että tietojen oikeellisuus on osoitettavissa.

ISO/IEC 27001 -standardia voidaan soveltaa eri organisaatiossa riippumatta niiden tyypistä, koosta tai luonteesta. Tyypillisesti ISO/IEC 27001 -standardin kohde ja kattavuus määritellään tarkasti organisaation luonteen perusteella, ja standardia sovelletaan kohteena olevaan organisaatioon, palveluun tai toimintoon. Kattavuudessa voidaan rajata pois tiettyjä standardin vaatimia turvamekanismeja perustellen ja huomioiden rajaukset organisaation riskien hallinnassa.

Turvamekanismien pois rajaamista tietoturvallisuuden hallintajärjestelmässä ei voida kuitenkaan hyväksyä suoraan standardien vaatimusten mukaisuuteen vedoten. Ainoa hyväksyttävä peruste pois rajaamiselle on, että asia ei vaikuta organisaation tietoturvallisuuteen, ja se täyttää riskien hallinnan ja lakisääteisten vaatimusten turvallisuusvaatimukset. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

ISO/IEC 27001 -standardi on osa ISO/IEC 27000 -standardiperhettä, joiden yhteinen otsikko on: ”Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät”. ISO/IEC 27001 -standardin uusin version on vuodelta 2005, ja se on ainoa osa standardiperheestä, johon voi sertifioitua. Standardiperheen osat ovat nykyisin seuraavat (Humphreys 2007, 11):

- ISO/IEC 27000:2009, Tietoturvallisuuden hallintajärjestelmät. Yleiskatsaus ja sanasto.
- ISO/IEC 27001:2005, Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.
- ISO/IEC 27002:2005, Tietoturvallisuuden hallintaa koskeva menettelyohje.
- ISO/IEC 27003:2010, Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita.
- ISO/IEC 27004:2009, Tietoturvallisuuden hallinta. Mittaaminen.
- ISO/IEC 27005:2008, Tietoturvariskien hallinta.
- ISO/IEC 27006:2007, Tietoturvallisuuden hallintajärjestelmien auditointiohjeet.

ISO/IEC 27001 on yhdenmukainen perusosiltaan muiden kansainvälisten standardien kuten ISO 9001:2000 ja ISO 14001:2004 kanssa. Yhteneväisyys mahdollistaa organisaatioille tuen eri hallintajärjestelmien yhteensovittamiseksi ja tarpeiden mukaan suunnitelluksi hallintajärjestelmäksi. Yhtenevät osa-alueet ISO/IEC 27001 -standardissa verrattuna muihin hallintajärjestelmiin ovat prosessimainen toimintamalli, jatkuva seuranta ja mittaus, asiakirjojen ja tallenteiden ohjaus ja hallinta, johdon vastuu ja sitoutuminen sekä säännölliset katsel-

mukset ja hallintajärjestelmän parantamiseen liittyvät toimenpiteet. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

3.1 Standardin vaatimukset

ISO/IEC 27001:2005 -standardien olennaisena osana on omaksua prosessimainen toimintamalli tietoturvallisuuden hallintajärjestelmän kehittämiseen, toteuttamiseen, käyttämiseen, valvomiseen, katselmointiin, ylläpitämiseen ja parantamiseen. Standardin pakollisia vaatimuksia riippumatta organisaation tyypistä tai luonteesta ovat standardin seuraavat osa-alueet: (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

- tietoturvallisuuden hallintajärjestelmä
- johdon vastuu
- tietoturvallisuuden hallintajärjestelmän sisäiset auditoinnit
- tietoturvallisuuden hallintajärjestelmän johdon katselmus
- tietoturvallisuuden hallintajärjestelmän parantaminen

Lisäksi organisaation tulee laatia soveltamissuunnitelma, jossa kuvataan tietoturvallisuuden hallintajärjestelmän kannalta olennaiset valvontatavoitteet ja turvamekanismit. Soveltamissuunnitelman valvontatavoitteet ja turvamekanismit perustuvat organisaation toiminnan asettamiin tietoturvavaatimuksiin, mahdollisiin sopimusvelvoitteisiin sekä riskien hallinnan tuloksiin ja päätelmiin ja lakisääteisiin vaatimuksiin. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Pakolliset vaatimukset on kuvattu tarkemmin seuraavissa kappaleissa.

3.1.1 Prosessimainen toimintamalli

Prosessimainen toimintamalli ISO/IEC 27001:2005 -standardissa perustuu PDCA-malliin, joka on organisaation johtamismalli toimintojen suunnitteluun,

kehittämiseen ja ohjaukseen. PDCA-malli koostuu neljästä eri tehtävästä, joita sovelletaan jatkuvana prosessina ISO/ IEC 27001 -standardin prosesseissa. (Moisio 2011).

Kuviossa 1 esitetään PDCA-mallin toteutuminen ISO/IEC 27001 -standardin osalta.

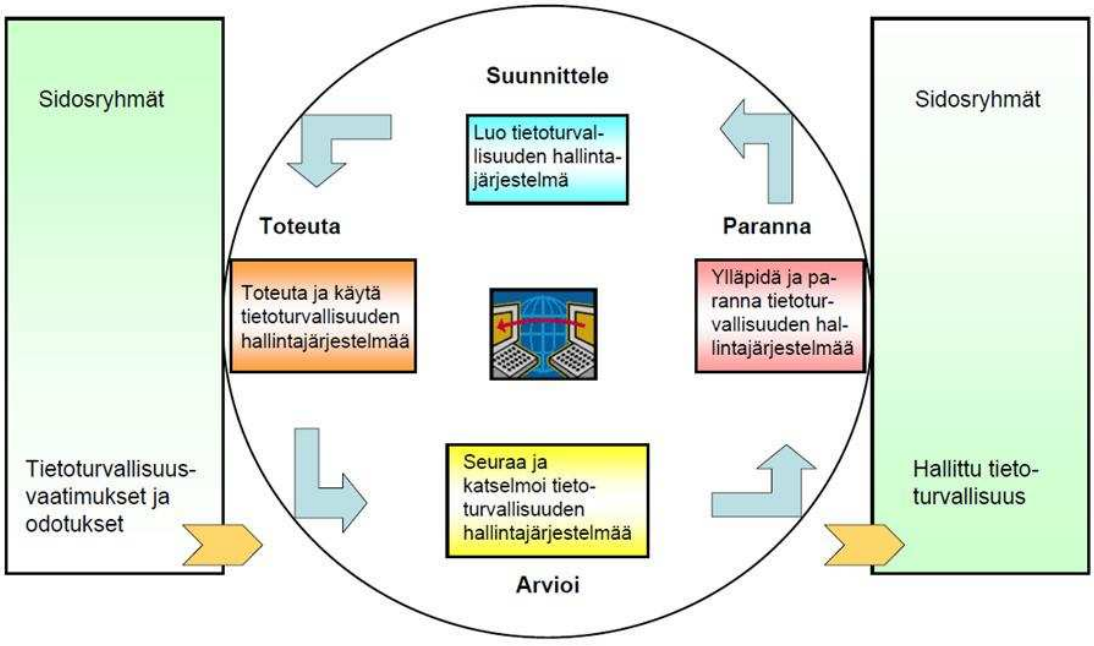
PDCA-malli muodostuu seuraavista osa-alueista:

P = Plan, Suunnitele

D = Do, Toteuta

C = Check, Arvioi

A = Act, Toimi



Kuvio 1: PDCA-malli ISO/IEC 27001 -standardissa (Moisio 2011).

Prosessimaisen toimintamallin avulla pyritään korostamaan tietoturvallisuuden hallinnassa seuraavia asioita:

- Organisaatio ymmärtää tietoturvavaatimukset ja määrittelee tietoturvapolitiikan ja tavoitteet.
- Turvamekanismeja luodaan ja käytetään organisaation tietoturvariskien hallintaan yleisten liiketoimintariskien puitteissa.
- Tietoturvallisuuden hallintajärjestelmää valvotaan ja sen suorituskykyä katselmoidaan säännöllisesti.
- Jatkuva parantaminen perustuu objektiiviseen mittaamiseen.

Seuraava taulukko kuvaa eri prosessien soveltamisen tietoturvallisuuden hallintajärjestelmässä:

Suunnittelu Luodaan tietoturvallisuuden hallintajärjestelmä	Luodaan ja määritellään tietoturvapolitiikka, tavoitteet, prosessit ja muut käytännöt, jotka ovat oleellisia organisaation muille poliitikoille, kehittämiselle, tavoitteille ja riskien hallinnalle.
Toteutus Toteutetaan ja käytetään tietoturvallisuuden hallintajärjestelmää	Toteutetaan ja käytetään luotua tietoturvapolitiikkaa, turvamekanismeja, prosesseja ja muita menettelytapoja.
Arviointi Seurataan ja katselmoidaan tietoturvallisuuden hallintajärjestelmää	Seurataan ja mitataan soveltaen prosessien suorituskykyä, ja vertaa tuloksia luotuihin politiikkoihin, käytäntöihin ja tavoitteisiin. Lisäksi raportoidaan tuloksista johdolle katselmointeja varten.
Toiminta Ylläpidetään ja parannetaan tietoturvallisuuden hallintajärjestelmää	Suoritetaan tarvittavat korjaavat ja ehkäisevät toimenpiteet sisäisten tietoturvallisuuden hallintajärjestelmän auditointien ja johdon katselmusten tulosten tai muiden olennaisten tietojen mukaisesti tietoturvallisuuden jatkuvaksi parantamiseksi.

(ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

3.1.2 Tietoturvallisuuden hallintajärjestelmä

ISO/IEC 27001 -standardin olennaisin osa on tietoturvallisuuden hallintajärjestelmän luominen, jonka avulla toteutetaan ja varmistetaan kappaleessa 3 esitetty tietojen luottamuksellisuus, eheys ja käytettävyys. Tietoturvallisuuden hallintajärjestelmän avulla pyritään takaamaan liiketoiminnan jatkuvuus sekä toisaalta minimoimaan tietoturvahäiriöitä ja niistä aiheutuvia seuraamuksia. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

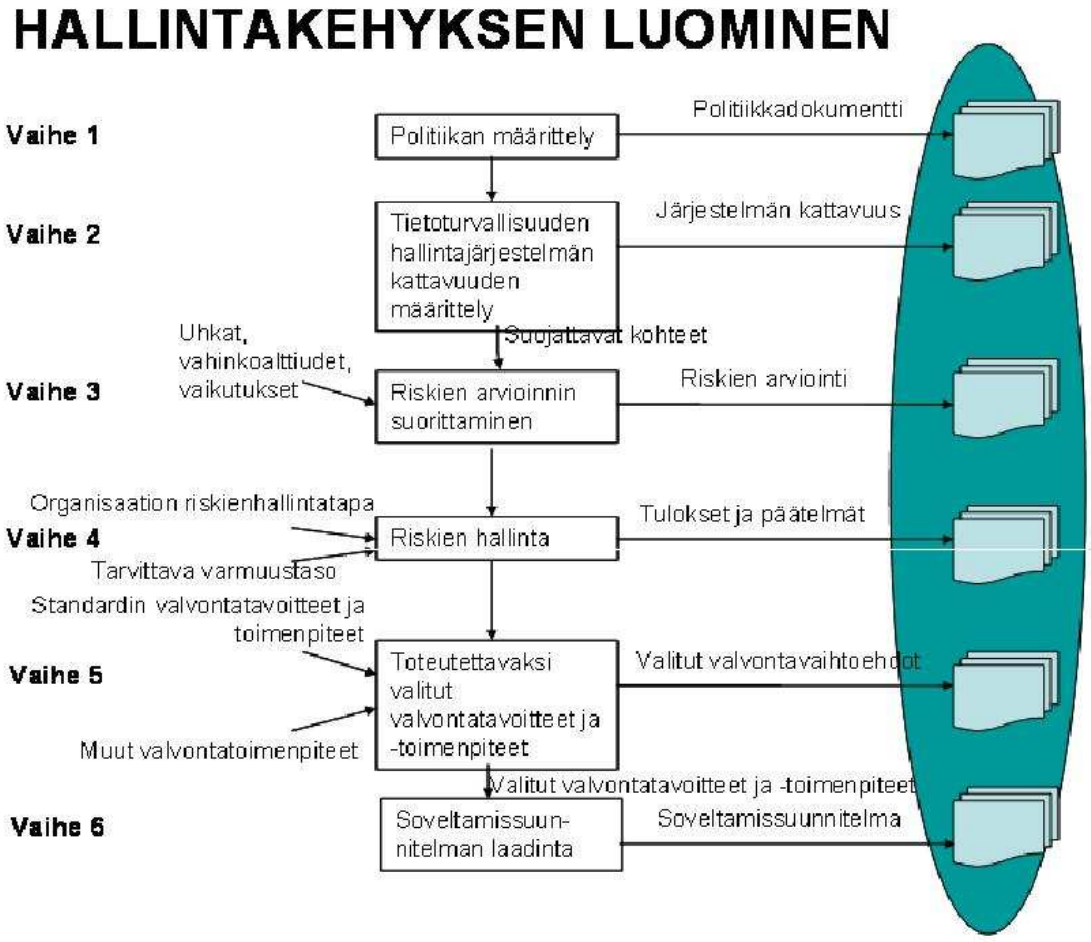
Tietoturvallisuuden hallintajärjestelmän luomisessa ja dokumentoinnissa on olennaista määritellä järjestelmän kattavuus ja rajat ottaen huomioon liiketoiminnan tarpeet. Lisäksi on otettava huomioon organisaatioon ja suojattaviin kohteisiin liittyvät erityispiirteet. Tietoturvallisuuden hallintajärjestelmä kattaa myös sopimukselliset, lainsäädännölliset sekä hallinnolliset vaatimukset tietoturvallisuudelle. Hallintajärjestelmän tulee olla johdon hyväksymä. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Tietoturvallisuuden hallintajärjestelmän olennaisia osia ovat organisaation tietoturvallisuuspolitiikka ja –tavoitteet, sekä riskien hallinnan toimintatavat ja menetelmät. Tietoturvallisuuden hallintajärjestelmän tulee koostua seuraavista dokumenteista:

- Organisaation tietoturvapolitiikan dokumentointi sisältäen tavoitteet, vastuut, toteutustavat, seurannan ja sanktioinnin.
- Hallintajärjestelmän kattavuus
- Hallintajärjestelmään liittyvät menetelmät, prosessit sekä turvamekanismit
- Riskien arvioinnin ja hallinnan menettelytavat ja suunnitelma
- Soveltamissuunnitelma

- Dokumentit joiden avulla organisaatio varmistaa tietoturvaprosessien suunnittelun, käytön ja valvonnan käyttöönotettujen turvamekanismien tehokkuuden mittaamiseksi
- Raportti riskien arvioinnista ja hallinnasta.

Seuraava kuvio 2 esittää tietoturvallisuuden hallintajärjestelmän luomisen vaiheet.



Kuvio 2: Hallintakehyksen luominen (ISO 27001 -koulutuksen luentomateriaali 2008).

3.1.3 Johdon vastuu

Johdon tulee osoittaa vastuunsa tietoturvallisuuden hallintajärjestelmän luomisessa, käytössä, valvonnassa ja kehittämisessä osoittamalla sitoutuminen, varaamalla resurssit sekä varmistamalla riittävä tietoturvallisuuteen liittyvä koulutus, tietoisuus ja pätevyys. Johdon sitoutumisen osalta olennaisia asioita on, määritellä tietoturvapolitiikka mahdollisimman kattavasti organisaation tarpeisiin. Johdon sitoutuminen on tärkeää, jotta voidaan varmistaa tietoturvallisuuden merkitys organisaation jokapäiväisessä toiminnassa. (ISO/IEC 27001 - tietoturvallisuusstandardi 2006).

Tietoturvapolitiikan tulee sisältää tietoturvallisuuteen liittyvät roolit ja vastuut, ja johdon vastuulla on, että tietoturvapolitiikka on viestitty asianmukaisesti koko organisaatiolle huomioiden lakisääteiset vaatimukset. Tietoturvapolitiikan tulee sisältää tietoturvatavoitteet. Johdon vastuulla on varmistaa, että tietoturvallisuuden ylläpitämiseksi on laadittu suunnitelmat. (Miettinen 1999, 104–108).

Johdon tulee varmistaa, että tietoturvallisuuden hallintajärjestelmää kehitetään jatkuvana prosessina sisäisten auditointien tulosten perusteella, ja tietoturvallisuuden hallintajärjestelmä on katselmoitu johdon toimesta. Johdon vastuulla on lisäksi päättää hyväksyttävät riskitasot ja riskien hyväksymiskriteerit. (Miettinen 1999, 108–115).

3.1.4 Sisäiset auditoinnit

ISO/IEC 27001 -standardi vaatii, että tietoturvallisuuden hallintajärjestelmää auditoidaan osana jatkuvaa prosessia. Sisäisten auditointien tarkoituksena on tarkistaa yhteensopivuus standardin vaatimuksia vasten, sekä luotuja toimintatapoja, päämääriä ja liiketoimintavaatimuksia vasten. Sisäisien auditointien avulla varmistetaan lisäksi, että riskien hallinnan menetelmät ovat tehokkaita, ne ovat toteutettu. (Tietojärjestelmien tarkastus ja valvonta ry. 1997).

Sisäisten auditointien menettelyt luovat lähtökohdat muutoksille, korjaaville ja ehkäiseville toimenpiteille, sekä tarjoaa johdolle arvion turvamekanismien toiminnasta. Sisäisissä auditoinneissa käsiteltäviä asioita ovat tietoturva-auditointien tulokset, tietoturvahäiriöt, tehokkuusmittausten tulokset sekä eri sidosryhmiltä saadut palautteet ja ehdotukset. (Tietojärjestelmien tarkastus ja valvonta ry. 1997).

Sisäiset auditoinnit jaetaan tyypillisesti seuraaviin osa-alueisiin:

- hallinto ja yhdenmukaisuus standardiin nähden
- prosessiauditoinnit
- palveluiden auditoinnit
- tietoturva-auditoinnit, kuten käyttöoikeuksien auditointi.

3.1.5 Johdon katselmus

ISO/IEC 27001 -standardi vaatii, että organisaation johdon on suoritettava johdon katselmukset tietoturvallisuuden hallintajärjestelmälle säännöllisesti. Standardin vaatimuksena on, että katselmukset suoritetaan vähintään kerran vuodessa. Katselmuksen tulee sisältää kokonaisuudessaan hallintajärjestelmän arvioinnin, mikä sisältää luodut tavoitteet, mittarit, tietoturvapolitiikan sekä mahdolliset muutos- ja kehitystarpeet. Katselmuksista on pidettävä yllä kattavaa dokumentointia. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Katselmuksia varten kerätään lähtötiedot tietoturvallisuuden hallintajärjestelmän sisäisten tai ulkoisten auditointien tuloksista ja sidosryhmien palautteista. Lähtötietoina käytetään myös aiempien katselmusten tuloksia, riskien hallinnan tuloksia. Tyypillisesti johdon katselmuksissa käsitellään seuraavia asioita:

- asiakastyytyväisyys ja asiakasreklamaatioiden tilanne
- hallintajärjestelmien mittareiden toteutuminen

- auditointiraportit
- korjaavien toimenpiteiden tilanne ja toteutuminen
- riskien hallinnan tilanne.

Katselmuksien tuloksina johdon täytyy tehdä päätökset ja toimenpiteet tietoturvallisuuden kehittämiseksi tai riskien hallinnan toimintatapojen muuttamiseksi. Tuloksina voivat olla myös mahdolliset resursointiin, tehokkuuden mittaamiseen ja menettelytapojen tai turvamekanismien muuttamiseen liittyvät toimenpiteet. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

3.1.6 Jatkuva parantaminen

Jatkuva parantaminen on oleellinen osa ISO/IEC 27001 -standardin mukaista prosessinomaista toimintaa sekä standardissa käytettävää PDCA-mallia. Jatkuvan parantamisen toimenpiteillä varmistetaan tietoturvallisuuden hallintajärjestelmän jatkuva kehittyminen. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Jatkuvan parantamisen toimenpiteet voivat käynnistyä riskien hallinnan tehtävistä, asiakaspalautteesta, sisäisistä tai ulkoisista auditoinneista tai organisaation henkilökunnan kehitysehdotuksista. Kaikki jatkuvaan parantamiseen liittyvät toimenpiteet tulee tallentaa korjaavien toimenpiteiden listaan. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Jatkuvan parantamisen toimenpiteitä ovat:

- korjaavien ja ehkäisevien toimenpiteiden suoritus sisäisten ja ulkoisten auditointien, mittaustulosten, johdon katselmusten sekä muiden palautteiden tiedoista
- tietoturvallisuuden hallintajärjestelmän testaustapahtumat

- organisaation henkilökunnan ja sidosryhmien säännöllinen koulutus
- tietoturvallisuuden hallintaan tarvittavien resurssien käytön ja osaamisen arvioinnit sekä muutokset
- uusien turvamekanismien luonti organisaation liiketoimintatarpeisiin
- viestintä organisaatiolle tietoturvallisuuteen liittyvistä asioista.

Tärkeintä jatkuvalle parantamiselle on, että tietoturvallisuuden toteutumista seurataan jatkuvana prosessina, ja mahdollisiin poikkeamiin puututaan välittömästi.

3.2 Valvontatavoitteet ja turvamekanismit

ISO/IEC 27001 -standardin olennaisena osana on standardin liitteen A mukaisten valvontatavoitteiden ja turvamekanismien käyttöönotto ja soveltaminen osana organisaation tietoturvallisuuden hallintajärjestelmää. Valvontatavoitteet koostuvat 11 eri valvontatavoitteiden osa-alueesta, joiden alla on kaiken kaikkiaan 133 turvamekanismia. Standardin valvontatavoitteiden ja turvamekanismien ei ole tarkoitus olla kaiken kattavia, vaan näiden lisäksi organisaatio voi luoda omia turvamekanismeja. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Valvontatavoitteiden ja turvamekanismien käyttö tulee kuvata osana soveltamissuunnitelmaa. Soveltamissuunnitelma sisältää lisäksi suojattavien kohteiden määrittelyn sekä riskien käsittelyn linkitettynä käytössä oleviin turvamekanismeihin mittareineen. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006). Valvontatavoitteiden osa-alueet on kuvattu seuraavissa kappaleissa.

3.2.1 Turvallisuuspolitiikka

Tietoturvallisuuspolitiikan tarkoituksena on kuvata ja määritellä asiat, miten organisaatio määrittelee tietoturvallisuuteen liittyvät käytännöt. Tietoturvallisuuspolitiikan tulee olla organisaation ylimmän johdon hyväksymä. Tietoturvallisuus-

politiikkaa tulee kehittää säännöllisesti, ja sen tulee olla viestitty kaikille sidosryhmille. Tietoturvallisuuspolitiikkaa tulee katselmoida säännöllisesti osana sisäisiä auditointeja. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Tietoturvallisuuspolitiikan ajatuksena on taata organisaatiolle tietoturvallisuustavoitteiden ohjaus ja tuki, sekä varmistaa se, että esimerkiksi liiketoimintatavoitteiden ja lakien sekä asetusten vaatimat tietoturvallisuusperiaatteet toteutuvat organisaatiossa. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

3.2.2 Tietoturvallisuuden organisoiminen

Tietoturvallisuuden organisoitumisen avulla varmistetaan, että tietoturvallisuus toteutuu organisaation sisällä sekä ulkoisten tahojen välillä. Määriteltyjen roolien avulla osoitetaan johdon sitoutuminen tietoturvallisuuden hallintaan. Vastuiden tulee olla selkeästi määriteltyjä, ja tietoturvallisuuden hallinnan kokonaisuuden tulee olla selkeästi koordinoitua. Lisäksi organisoitumisen avulla varmistetaan riittävät yhteydet esimerkiksi viranomaistahoihin tai muihin erityisryhmiin. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Organisoitumisen avulla varmistetaan ja ylläpidetään lisäksi organisaation tietojen ja tietojenkäsittelypalveluiden turvallisuutta tilanteissa, joissa ulkoiset sidosryhmät pääsevät käsittelemään, näkemään tai hallinnoimaan organisaation tietoja. Yhteistyöllä sertifiointeja suorittavien tahojen avulla varmistetaan, että organisaation tietoturvallisuuden on arvioitu puolueettomasti ja riippumattomasti. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

3.2.3 Suojattavien kohteiden hallinta

Suojattavien kohteiden hallinnan avulla määritellään organisaation suojattavat kohteet, ja varmistetaan, että ne ovat suojattuja ja ylläpidettyjä riittävin keinoin. Suojattavista kohteista tulee pitää ajantasaista luetteloa omistajineen. Suojatta-

ville kohteille tulee määritellä lisäksi hyväksyttävän käytön periaatteet. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Suojattavat kohteet ja tiedot tulee luokitella niiden kriittisyyden, luottamuksellisuuden sekä laki- ja asetusvaatimusten mukaisesti. Luokittelun avulla varmistetaan, että järjestelmissä, palveluissa tai dokumenteissa olevilla tiedoilla on riittävä suojaus. Tiedot tulee lisäksi merkitä organisaation luokittelutapojen mukaisesti, ja organisaation tulee laatia ohjeistus luokittelulle. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

3.2.4 Henkilöstöturvallisuus

Henkilöstöturvallisuuden tavoitteena ISO/IEC 27001 -standardissa on varmistaa, että organisaation työntekijät tai ulkoiset sidosryhmät ymmärtävät vastuunsa organisaation tietoturvallisuudessa koko työ- tai palvelusuhteen elinkaaren ajan. Henkilöstöturvallisuus määrittelee kaikkien sidosryhmien roolit ja vastuut tietoturvallisuudessa. Roolit, vastuut ja velvoitteet tulee kirjata sopimuksien muodossa eri sidosryhmien kanssa. Sopimuksien tulee sisältää myös seuraamukset mahdollisista tietoturvarikkomuksista. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Henkilöstöturvallisuuden avulla varmistetaan, että tietoturvallisuus toteutuu ennen palvelusuhteen alkamista, sen aikana sekä palvelusuhteen muuttuessa tai päättyessä. Henkilöstöturvallisuuden konkreettisia esimerkkejä ovat mm. sopimukset työntekijöiden ja eri sidosryhmien välillä, salassapitosopimukset sekä käyttöoikeuksien poistoon liittyvät tehtävät. Henkilöstöturvallisuus ehkäisee muun muassa varkauksien, petosten ja palveluiden väärinkäytön riskejä, sekä vähentää inhimillisten erehdysten riskejä. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

3.2.5 Fyysinen turvallisuus ja ympäristön turvallisuus

Fyysinen turvallisuus ja ympäristön turvallisuus standardissa jakaantuu kahteen osa-alueeseen, jotka voidaan mieltää toimitilojen ja turva-alueiden fyysiseen suojaukseen sekä laitteistojen turvallisuuteen. Näiden tarkoituksena on estää muun muassa luvaton pääsy toimitiloihin tai tietoihin sekä estää näiden vahingoittuminen ja häiriintyminen. Lisäksi pyrkimyksenä on varmistaa fyysisen omaisuuden häviäminen, vahingoittuminen, varastaminen tai muu vaarantuminen. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Fyysinen ja ympäristöturvallisuus vaatii, että organisaatio suojaa toimitilansa asianmukaisesti pääsynhallinnalla ja valvonnalla sekä varmistaa, että organisaatio on varautunut ympäristöstä aiheutuviin uhkiin. Ympäristöstä johtuvia uhkia ovat esimerkiksi eri luonnonilmiöistä aiheutuvat seuraamukset. Pääsynhallinnan ja valvonnan osalta konkreettisia esimerkkejä ovat muun muassa kulunvalvonnan ja videovalvonnan toteutukset. (Miettinen 2002, 91-100).

Laiteturvallisuus määrittelee organisaatiolle ne käytännöt joilla suojataan tietojenkäsittelyyn liittyvät laitteet. Laiteturvallisuuden osalta tulee huomioida, että laitteistoja huolletaan säännöllisesti käytettävyyden ja eheyden säilyttämiseksi. Laitteistot tulee sijoittaa siten, että niihin ei kohdistu vaaraa väärinkäytöksistä, vaurioista tai jopa salakuuntelulta. Laitteistoturvallisuuden avulla suojataan myös organisaation toimitilojen ulkopuolella liikkuvat laitteet ja niissä olevat tiedot. Lisäksi laiteturvallisuus varmistaa, jotta poistuvista laitteista on tuhottu turvallisesti kaikki suojattava tai tekijänoikeuden alainen materiaali. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

3.2.6 Tietoliikenteen ja käyttötoimintojen hallinta

Tietoliikenteen ja käyttötoimintojen hallinnan tarkoituksena on varmistaa, että organisaation tietojärjestelmiä käytetään asianmukaisesti ja tietoturvallisesti, jotta voidaan ehkäistä tietojen luvatonta käyttöä sekä muuttumista. Käytännös-

sä tämä toteutetaan kirjallisten menettelyohjeiden, muutosten hallinnan sekä tuotanto- ja kehitysympäristöjen eriyttämisen avulla. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Myös ulkopuolisten sidosryhmien tuottamia palveluita, raportteja ja tallenteita tulee valvoa ja katselmoida jatkuvana prosessina. Ulkopuolisten sidosryhmien tuottamien palveluiden tietoturvallisuus varmistetaan tehtävien sopimusten avulla, ja niihin sisällytettävien turvamekanismien kautta. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Tietojärjestelmien resursseja tulee valvoa riittävän kapasiteetin takaamiseksi. Kapasiteetin hallinnan avulla ennakoidaan myös tulevia resurssitarpeita sekä tarvittavia muutoksia, jotta voidaan varmistaa tietojärjestelmien häiriintymätön toiminta. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Uusien järjestelmien käyttöönottoon, järjestelmiin tehtäviin päivityksiin ja vaikka uusien ohjelmistoversioiden käyttöönottoon pitää luoda hyväksyntäkriteerit ja riittävät testaukset. Käytännössä tämä on luontevinta sitoa osaksi organisaation muutoksen hallintaprosessia. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Haitallisten ohjelmistojen, liikkuvien ohjelmistojen sekä virusten torjuntaan on luotava havainto- ja estotoimenpiteet sekä näiden osalta on laadittava toipumismekanismit. Oleellista on, että organisaation käyttäjät on opastettu noudattamaan riittävää valppautta haitallisten ohjelmistojen suhteen. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Tietoliikenneverkkojen suojaus, hallittavuus ja valvonta ovat olennainen osa tietojärjestelmäinfrastruktuurin suojauksen varmistamista. Verkkoja ja verkkopalveluita tulee hallita ja valvoa riittävästi riippumatta siitä ovatko ne organisaation sisäisiä tai ulkoistettuja. Ulkoistettujen palveluiden osalta turvamekanismien

toteutuminen tulee edellyttää sopimuksissa. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Siirrettävien medioiden käyttöön ja turvaamiseen tulee laatia toimintatavat sekä yleisesti käytöstä poistuvien välineiden ja järjestelmien poisto tulee suorittaa turvallisella ja luotettavalla tavalla. Tietojen tallennuksen, järjestelmien dokumentoinnin ja käsittelyn menettelytavat tulee luoda siten, että organisaatio pystyy varmistumaan tietojen väärinkäytöltä ja toisaalta ehkäisemään näiden luvattoman käytön. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Organisaation sisäisten ja ulkoisten sidosryhmien väliseen tietojen vaihtoon pitää suunnitella, ja dokumentoida tiedonvaihtoperiaatteet ja –menettelytavat sekä riittävät turvamekanismit. Tiedon vaihtoa tulee kontrolloida sopimuksien avulla. Suojaukset on määriteltävä koskemaan sekä tietojen fyysistä että sähköistä kuljetusta ja viestintää, jotta voidaan varmistua tietojen oikeellisuudesta sekä poistaa riskit tietojen väärinkäytöksiltä tai tuhoutumiselta. Vaatimukset koskevat organisaation liiketoiminnan järjestelmiä sekä sähköiseen viestintään käytettäviä järjestelmiä ja verkkoasioinnin järjestelmiä. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Olennainen osa tietoliikenteen ja käyttötoimintojen hallintaa on järjestelmien valvonta ja tarkkailu, joiden avulla pyritään havaitsemaan järjestelmissä tapahtuvat luvattomat toimet. Valvontaa varten kaikista järjestelmistä on kerättävä lokitietoa, joihin tallennetaan käyttäjien toiminta, poikkeamat ja tietoturvatapahtumat mahdollisia selvityksiä varten. Lokitietojen osalta on tärkeää, että ne ovat suojattuja muokkaukselta ja luvattomalta pääsyltä. Pääkäyttäjien toimet tulee kirjata myös lokitapahtumiin. Lokitietoja tulee säilyttää organisaation tietoturvapolitiikan mukainen määrätty aika, ja järjestelmien kellonajat tulee olla synkronoituja aikapalveluista lokitietojen oikeellisuuden varmistamiseksi. (Kuusela & Ollikainen 1999, 240-241).

3.2.7 Pääsyoikeuksien valvonta

Pääsyoikeuksien valvonnan ajatuksena on valvoa ja säädellä käyttäjien pääsyä suojattaviin kohteisiin. ISO/IEC 27001 -standardi vaatii, että pääsynvalvonnan toimintatavat ovat laadittu, dokumentoitu ja katselmoitu liiketoiminta- ja tietoturvallisuusvaatimusten mukaisesti. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Pääsyoikeuksien valvontaan liittyvän käyttöoikeuksien hallinnan avulla varmistetaan, että vain valtuutetut käyttäjät pääsevät tietojärjestelmiin, ja että käyttäjät ymmärtävät vastuunsa ja velvollisuutensa. Käyttöoikeuksien hallintaprosessi tulee olla kuvattuna, ja prosessia sekä oikeuksia tulee valvoa säännöllisesti. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Standardin vaatimukset pääsyn valvonnan osalta kohdistuvat verkkoon pääsyyn, käyttöjärjestelmiin pääsyyn sekä sovelluksiin ja tietoihin pääsyyn. Oleellista on, että käyttäjillä tarjotaan pääsy vain kohteisiin ja tietoihin, joihin he ovat oikeutettuja. Pääkäyttäjien oikeuksien myöntämistä tulee rajoittaa ja valvoa, sekä toisaalta niiden käyttöä tulee seurata. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Pääsyoikeuksien hallinnassa huomioidaan lisäksi mahdollinen etä- tai matkakäyttö tietoliikenteen, palveluiden ja järjestelmien osalta. Valvomattomien laitteiden osalta tulee varmistaa riittävä suojaus sekä organisaation tulee noudattaa niin kutsuttua ”puhtaan pöydän ja näytön politiikkaa”. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

3.2.8 Tietojärjestelmien hankinta, kehitys ja ylläpito

Tietotojärjestelmien hankinnan, kehityksen ja ylläpidon tarkoituksena on turvata organisaation tietojärjestelmien, sovellusten ja niissä olevien tietojen suojaus

niiden koko elinkaaren ajan käytöstä poistoon saakka. Standardi vaatii lisäksi, että kehitys- ja tukiprosessit ovat turvallisia. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Tietojärjestelmien hankinnan, kehityksen tai ylläpidon yhteydessä organisaation tulee huomioida uusien tai olemassa olevien järjestelmien tietoturvallisuusvaatimukset liiketoiminnalle. Järjestelmissä olevien tietojen suojaukseen, eheyden varmistamiseen sekä valvontaan tulee luoda menetelmät. Näiden menetelmien avulla varmistetaan, että tietojärjestelmät on kehitetty turvallisiksi, ja niissä olevat tiedot on suojattu virheiltä, katoamiselta sekä luvattomalta muuttamiselta ja väärinkäytöltä. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Standardi vaatii myös tietojärjestelmien osalta salakirjoitusmekanismien käyttöä sekä yleisiä periaatteita niiden käytölle. Salakirjoitusmekanismien tarkoituksena on suojata tietojen luottamuksellisuus, alkuperä ja eheys. (Allen 2002, 31).

Kehityksen osalta vaaditaan, että testiaineistot on valittu huolellisesti, ja ne ovat suojattuja ja valvottuja. Lisävaatimuksia ovat teknisten haavoittuvuuksien valvonta ja reagointi sekä ohjelmistojen lähdekoodien suojaus. Kehityksen osalta muutoshallintaprosessissa tulee huomioida muutosten jälkeinen tekninen testaus ja tarkastus, ja toisaalta esimerkiksi ohjelmistopaketteihin tehtävät muutokset tulee rajoittaa vain tarpeellisiin muutoksiin riskien hallitsemiseksi. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

3.2.9 Tietoturvahäiriöiden hallinta

Tietoturvahäiriöiden hallinnan tarkoituksena on luoda mekanismit sekä varmistaa, että mahdollisista heikkouksista ja haavoittuvuuksista viestitään, ja korjaaviin toimenpiteisiin ryhdytään riittävän ajoissa. Tietoturvahäiriöiden raportointia varten organisaatioissa tulee olla kuvattuna menetelmät ja toimintatavat, ja näi-

den tulee koskea kaikkia sidosryhmiä. Lisäksi standardi vaatii, että mahdollisista tietoturvahäiriöistä kerätään todistusaineistoa mahdollista jatkokäsittelyä varten lainsäädäntö ja asetukset huomioiden. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Tietoturvahäiriöistä oppimiseen tulee lisäksi luoda menettelytavat. Menettelytapojen avulla seurataan tietoturvahäiriöiden tyyppejä, määrää sekä niistä mahdollisesti seuraavia kustannuksia, jotta mahdollisia korjaavia ja ehkäiseviä toimintatapoja tai turvamekanismeja voidaan luoda. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

3.2.10 Liiketoiminnan jatkuvuuden hallinta

Liiketoiminnan jatkuvuuden hallinnan tarkoituksena on kuvata toiminta, jolla organisaatio varmistaa päivittäiset toimintonsa vakavassa häiriötilanteessa. Standardin vaatimuksena on, että organisaatiolla on oltava luotuna ja ylläpidettynä selkeä suunnitelma liiketoiminnan jatkuvuudesta. Liiketoiminnan jatkuvuussuunnitelmassa tulee kuvata organisaation liiketoimintaprosessit keskeyttävät tapahtumat, sekä niiden todennäköisyys, vaikutus ja seuraukset tietoturvallisuuden kannalta. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Liiketoiminnan jatkuvuussuunnittelu edellyttää organisaatiolta jatkuvaa prosessia keskeyttävien tapahtumien analysointiin sekä riskien arviointiin ja hallintaan. Prosessin tarkoituksena on ehkäistä toimintojen keskeytyminen, ja suojata liiketoimintaprosesseja ja tietojärjestelmiä muun muassa häiriöiden ja onnettomuuksien tai muiden uhkien osalta. Riskien hallinta ja arvioinnin menetelmät ovat olennaisia osia liiketoiminnan jatkuvuudelle, joiden avulla arvioidaan poikkeavien tapahtumien todennäköisyyttä ja vaikutusta organisaation toimintaan. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

3.2.11 Vaatimustenmukaisuus

Vaatimustenmukaisuus varmistaa organisaation yleisen toiminnan ja tietoturvallisuuden osalta, että organisaatio noudattaa sitä koskevia lakeja, asetuksia ja säännöksiä toiminnassaan. Vaatimustenmukaisuus listaa sovellettavat lainsäädökset, ja varmistaa, että organisaatiolla on asianmukaiset menetelmät käytössään muun muassa tekijänoikeuden alaisten tietojen käsittelyyn, organisaation tallenteiden suojaukseen, tietosuojaan ja yksityisyyteen, väärinkäytön estämiseen ja salakirjoitusmekanismeihin lainsäädännön ja asetusten mukaisesti. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

Osana vaatimustenmukaisuutta vaaditaan, että organisaatio noudattaa luotua tietoturvallisuuspolitiikkaa ja standardeja sekä teknisiä tarkastusmenetelmiä muun muassa tietojärjestelmille. Tietojärjestelmien tarkistuksen osalta organisaatiolla tulee olla käytössään tarkastusmenetelmät sekä niiden suojaamiseen liittyvät käytännöt. (ISO/IEC 27001 -tietoturvallisuusstandardi 2006).

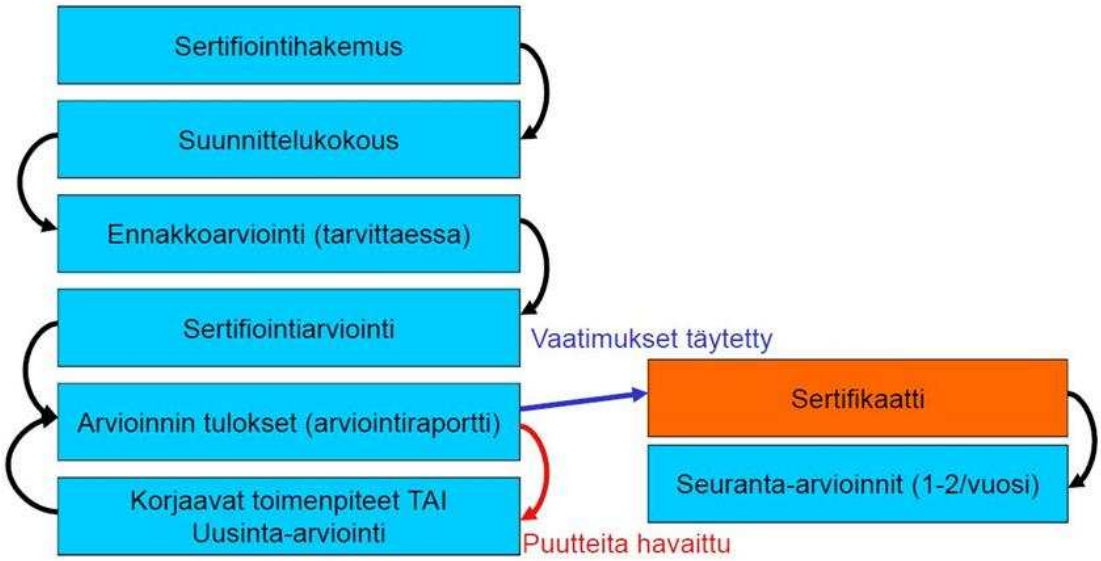
4 SERTIFIOINTI

Sertifiointi on menettely, jolla tunnistettu, riippumaton ja puolueeton kolmas osapuoli antaa kirjallisen varmistuksen siitä, että tuote, menetelmä tai palvelu on määriteltyjen vaatimusten mukainen. Sertifiointi on kansainvälisten ja kansallisten standardien ja vaatimustenmukaisuuden arviointia. Sertifiointia ISO-standardeihin tarjoavat Suomessa Suomen mittatekniikan keskuksen alaisen FINAS (Finnish Accrediation Service) akreditoimat yritykset kuten Inspecta ja Bureau Veritas.

4.1 Sertifiointiprosessi

Sertifiointiprosessi ISO/IEC 27001 -standardissa, kuten muissakin ISO-standardeissa, alkaa sertifiointihakemuksella sertifiointia suorittavalle taholle.

Sertifiointiprosessin vaiheet ovat seuraavat, ja ne ovat myös esitetty vaiheittain kuviossa 3. (ISO 27001 -koulutuksen luentomateriaali 2008).



Kuvio 3: Sertifiointiprosessi (ISO 27001 -koulutuksen luentomateriaali 2008).

Sertifiointihakemus

Sertifiointihakemuksessa kuvataan organisaation toiminta, jolle sertifikaattia tullaan hakemaan mahdollisine rajauksineen. Hakemus sisältää lisäksi perustiedot organisaatiosta, prosesseista, aikaisemmista sertifioinneista sekä organisaatiota koskevat lait, määräykset ja asetukset. (ISO 27001 -koulutuksen luentomateriaali 2008).

Suunnittelukokous

Sertifiointihakemuksen jälkeen seuraava vaihe sertifiointiprosessissa on suunnittelukokous yhdessä sertifioijan kanssa, minkä yhteydessä käydään läpi organisaation tietoturvallisuuden tai laadun hallintajärjestelmän dokumentaatio kokonaisuudessaan. Tyypillisesti hallintajärjestelmän materiaalit on luovutettava sertifioijalle tutustumista varten jo ennen suunnittelukokousta. (ISO 27001 -koulutuksen luentomateriaali 2008).

Suunnittelukokouksessa selvitetään viimeistään sertifioitavan järjestelmän rajaus ja kattavuus, sekä siihen liittyvät prosessit ja toimipaikat. Lisäksi suunnittelukokouksessa arvioidaan johdon katselmusten ja sisäisten auditointien käytännöt ja tilanne. Mikäli organisaatiolla on jo jokin muu sertifioitu hallintajärjestelmä, uuden järjestelmän osalta käydään läpi mahdolliset jo aiemmin arvioidut ja yhtenevät osa-alueet, joita ei tarvitse arvioida uudelleen yksityiskohtaisesti, kunhan yhteys uuteen järjestelmään on selkeästi olemassa ja osoitettavissa. (ISO 27001 -koulutuksen luentomateriaali 2008).

Ennakkoarviointi

Ennakkoarviointi on vapaaehtoinen ja se toteutetaan kuten sertifiointiarviointi, mutta suppeampana. Ennakkoarvioinnin laajuus määritellään yhdessä sertifioijan ja sertifikaattia hakevan organisaation välillä. Ennakkoarvioinnissa todettujen poikkeamien korjaavia toimenpiteitä ei tarvitse lähettää sertifioijalle. Ennakkoarviointi ei korvaa varsinaista sertifiointiarviointia miltään osin. Ennakkoarvioinnin ajatuksena on kuvata organisaatiolle sen valmiudet varsinaiseen sertifiointiarviointiin. (ISO 27001 -koulutuksen luentomateriaali 2008).

Sertifiointiarviointi

Varsinainen sertifiointiarviointi suoritetaan etukäteen luodun arviointiohjelman mukaisesti. Sertifiointiarvioinnin ideologiana on saada riittävä näyttö siitä, että organisaation toiminta vastaa luotuja hallintajärjestelmän kuvauksia ja standardin vaatimuksia. Sertifiointiarvioinnin päätteeksi organisaation hallintajärjestelmän osalta todetaan arvioinnin tulos. Arvioinnista vastuussa oleva sertifiointiarvioija kertoo arvioinnin tulokset sekä sen, voidaanko sertifikaatin myöntämistä suositella, tarvitaanko korjaavia toimenpiteitä tai uusinta-arviointia. Arvioinnin päätteeksi organisaatio saa kirjallisen arviointiselosteen ja poikkeamaraportit. (ISO 27001 -koulutuksen luentomateriaali 2008).

Poikkeamat sertifiointiarvioinnissa luokitellaan lieviin ja vakaviin.

Vakavia poikkeamia ovat:

- jokin standardin edellyttämä oleellinen asia on kuvaamatta tai puuttuu kokonaan
- jokin standardin kohtaa vastaan tai jossakin toiminnossa on todettu monta lievää poikkeamaa
- järjestelmä todetaan olennaisilta osilta keskeneräiseksi.

Lieviä poikkeamia ovat yksittäiset puutteet menettelyissä tai toiminnassa.

Organisaation tulee lähettää sertifioijalle määräajan kuluessa selvitys poikkeamien korjaavista toimenpiteistä. Määräaika sovitaan arviointiraportin luovutuksen yhteydessä. Sertifioijalle tulee toimittaa raportti korjaavien toimenpiteiden osalta seuraavista asioista:

- mitkä asiat on muutettu
- miten ohjeita on muutettu ja uudet ohjeistukset
- milloin muutokset astuvat voimaan
- miten muutoksista on tiedotettu
- miten muutokset estävät vastaavien poikkeamien uusiutumisen
- ketkä ja milloin ovat tarkastaneet muutoksien tai korjauksien toteutumisen.

Sertifioija tulee tarkastamaan korjaavien toimenpiteiden tehokkuuden toteutumisen. Korjaavien toimenpiteiden luonteesta riippuen tarkastaminen tehdään joko lähetetyn kirjallisen aineiston perusteella tai uusinta-arvioinnin yhteydessä. (ISO 27001 -koulutuksen luentomateriaali 2008).

Uusinta-arviointi

Uusinta-arviointi tehdään vakavien poikkeamien korjaavien toimenpiteiden todentamiseksi. Uusinta-arvioinnissa arvioidaan korjaavien toimenpiteiden toteu-

tuminen ja tehokkuus sekä ne järjestelmän osat, joihin tehdyt muutokset ovat saattaneet vaikuttaa. Jos järjestelmä on todettu sertifiointiarvioinnissa keskeneräiseksi, uusinta-arviointi tehdään laajempana. (ISO 27001 -koulutuksen luentomateriaali 2008).

Seuranta-arvioinnit

Sertifikaatin myöntämisen jälkeen seuranta-arviointeja suoritetaan vähintään kerran vuodessa seuraavien vaihtoehtojen mukaisesti, joista organisaatio voi valita sopivimman vaihtoehdon alla olevan listan mukaisesti: (ISO 27001 -koulutuksen luentomateriaali 2008).

1. Seuranta-arviointi tehdään kerran vuodessa ja niissä arvioidaan järjestelmän kriittisimmät kohteet ja muutokset. Ensimmäinen seuranta-arviointi tehdään viimeistään 12 kuukauden kuluttua sertifiointiarvioinnista.

2. Seuranta-arviointeja tehdään kaksi kertaa vuodessa. Arviointien sisältö sovitaan vuosittain yhdessä organisaation kanssa. Ensimmäinen seuranta-arviointi tehdään 6 kuukauden kuluttua sertifiointiarvioinnista.

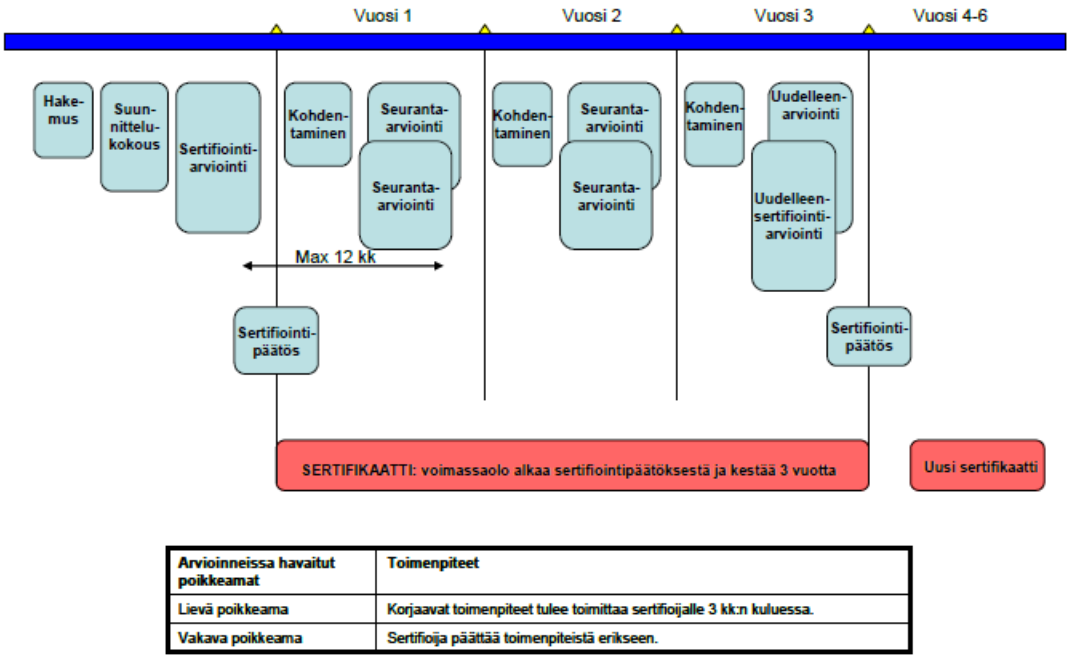
3. Jatkuva seuranta-arviointi, jolloin arviointien sisältö sovitaan vuosittain yhdessä organisaation kanssa. Sopii erityisesti isoille organisaatioille, jolloin yhdellä kertaa tehtävät arviointikäynnit ovat kohtuullisen kokoisia.

Ylimääräinen seuranta-arviointi tehdään, jos siihen sertifioijan mielestä on aihetta tai jos organisaatio sitä pyytää.

Jos sertifioija on sertifioinut organisaation muita hallintajärjestelmiä, eri järjestelmien seuranta-arvioinnit voidaan yhdistää, mikäli hallintajärjestelmiä voidaan käsitellä kokonaisuutena. (ISO 27001 -koulutuksen luentomateriaali 2008).

Seuranta-arviointikäyntien ajankohdat sovitaan organisaation kanssa etukäteen. Seuranta-arviointi raportoidaan kuten sertifiointiarviointi. Jos siinä todetaan vakava poikkeama, sertifioija käsittelee asian tapauskohtaisesti ja tekee siitä päätöksen. Päätös voi olla uusinta-arviointi, sertifikaatin määräaikainen peruuttaminen tai peruuttaminen kokonaan. (ISO 27001 -koulutuksen luentomateriaali 2008).

Sertifioinnin elinkaari on esitetty kuviossa 4.



Arvioinneissa havaitut poikkeamat	Toimenpiteet
Lievä poikkeama	Korjaavat toimenpiteet tulee toimittaa sertifioijalle 3 kk:n kuluessa.
Vakava poikkeama	Sertifioija päättää toimenpiteistä erikseen.

Kuvio 4: Sertifioinnin elinkaari (ISO 27001 -koulutuksen luentomateriaali 2008).

5 CASE-YRITYS

Cygate Oy on pohjoismaiden johtava turvallisten ja hallittavien tietoverkkoratkaisuiden toimittaja. Yhtiö on perustettu vuonna 1989, jolloin toiminta keskittyi laajalti pelkästään tietoliikennetuotteiden jälleenmyyntiin sekä asiantuntijapalveluihin. Nykyisin Cygate suunnittelee, asentaa ja ylläpitää sekä valvoo ja hallitsee IP-teknologiaan perustuvia tietoverkkoratkaisuja. Cygaten liiketoiminta jakaantuu tuotemyyntiin, asiantuntijapalveluihin sekä käytettävyyspalveluihin.

Cygaten käytettävyyspalvelut -liiketoiminta muodostuu jatkuvista tietoliikenne- ja tietoturvaympäristöjen valvonta- ja hallintapalveluista sekä ylläpitopalveluista. Cygaten käytettävyyspalvelut -yksikkö tarjoaa asiakkailleen kellon ympäri vuoden jokaisena päivänä valvontaa ja hallintaa verkkolaitteille, tietoturvalaitteille sekä tarvittaessa palvelimille ja sovelluksille.

Cygate on osa Cygate Group -konsernia. Cygate Group -konserni toimii sekä Suomessa että Ruotsissa, ja konsernin omistaa Teliasonera. Cygate Group -konsernissa on kaikkiaan n. 550 työntekijää, joista n. 110 työskentelee Cygate Oy:ssä. Cygate Oy:n liikevaihto vuonna 2010 oli n. 35,98 miljoonaa euroa. Vuoden 2012 alussa Cygate yhdistyy Crescom Oy:n kanssa.

5.1 Lähtökohdat ja tavoitteet

Lähtökohtana ISO/IEC 27001 -standardin ja tietoturvallisuuden hallintajärjestelmän käyttöönotolle ja kehitysprojektin käynnistykselle Cygate Oy:ssä oli Cygaten asiakkaiden vaatimukset tietoturvallisuudelle. Monet Cygaten asiakkaista edellyttävät yhteistyökumppaniltaan tietoturvallisuuden osoittamista sertifioinnin kautta, mikä on puolueeton tapa osoittaa tietoturvallisuuden toteutuminen.

Cygaten johto on lisäksi määritellyt tietoturvallisuuden merkittäväksi osaksi myös yrityksen strategiaa ja tietoturvallisuutta, ja on sitoutunut kehittämään yrityksen laatua. Cygaten tietoturvallisuusperiaatteissa on määritelty tietoturvallisuuden tavoitteiksi seuraavat asiat:

1. Cygate on luotettava palveluntarjoaja ja kumppani.
2. Cygaten omaisuus, palvelut ja tiedot ovat suojassa.
3. Cygaten haltuun uskottujen asiakkaiden ja kumppaneiden tietoja käsitellään ja säilytetään luottamuksellisesti.

4. Tietoturvallisuustoimenpiteet ovat liiketoimintalähtöisiä, Cygaten strategiaa ja arvoja tukevia tai lakeihin ja säädöksiin perustuvia.
5. Cygaten oma ja asiakkaiden turvallinen ja häiriötön liiketoiminta on varmistettu sekä vahinkomahdollisuudet minimoitu.
6. Liiketoiminnan ja uusien palvelujen kehittämisessä sekä kaikissa projekteissa ja tehtävissä huomioidaan tietoturvallisuus.
7. Tietoturvaratkaisut suunnitellaan ja toteutetaan riskiarviointiin perustuen. Ratkaisut dokumentoidaan ja toimivuus todennetaan.
8. Tietoturvatietoisuutta kehitetään ja käyttäjiä kannustetaan tietoturvatietoiseen käyttäytymiseen.
9. Tietoturvallisuus on osa Cygaten laadunhallintajärjestelmää, ja tietoturvallisuuden hallinnassa noudatetaan ISO/IEC 27001:2005 vaatimia periaatteita.
10. Tietoturvallisuuden toteutumista ja riittävyyttä mitataan säännöllisesti osana ISO/IEC 27001:2005 vaatimuksia.

Näiden tavoitteiden mukaisesti Cygatessa päätettiin käynnistää projekti johdon toimeksiantona, jonka tarkoituksena oli valmistella yritys ISO/IEC 27001 standardin käyttöönottoon ja sertifiointiin Cygaten jatkuvien palveluiden osalta eli Cygaten käytettävyyspalveluiden osalta. ISO/IEC 27001 -standardin käyttöönoton yhteydessä päätettiin lisäksi aloittaa yrityksen käytettävyysliiketoiminnan osalta valmistautuminen ISO/IEC 20000 -standardin mukaiseen toimintaan ja sertifiointiin. ISO/IEC 20000 on kansainvälinen standardi tietotekniikkapalveluiden johtamiseen ja hallintaan. Tätä standardia ei käsitellä tässä kehitystyössä.

6 KEHITYSPROJEKTI

Cygatessa käynnissä olleen kehitysprojektin tavoitteena oli arvioida Cygaten käytettävyyspalveluiden osalta tietoturvallisuuden nykytila standardin vaatimuksiin nähden sekä valmistella yrityksen toiminta ISO/IEC 27001 -standardin vaatimuksiin toiminnan ja dokumentoinnin osalta, sekä saattaa dokumentaatio ja toimintamallit mahdollisimman valmiiksi standardin sertifiointia varten.

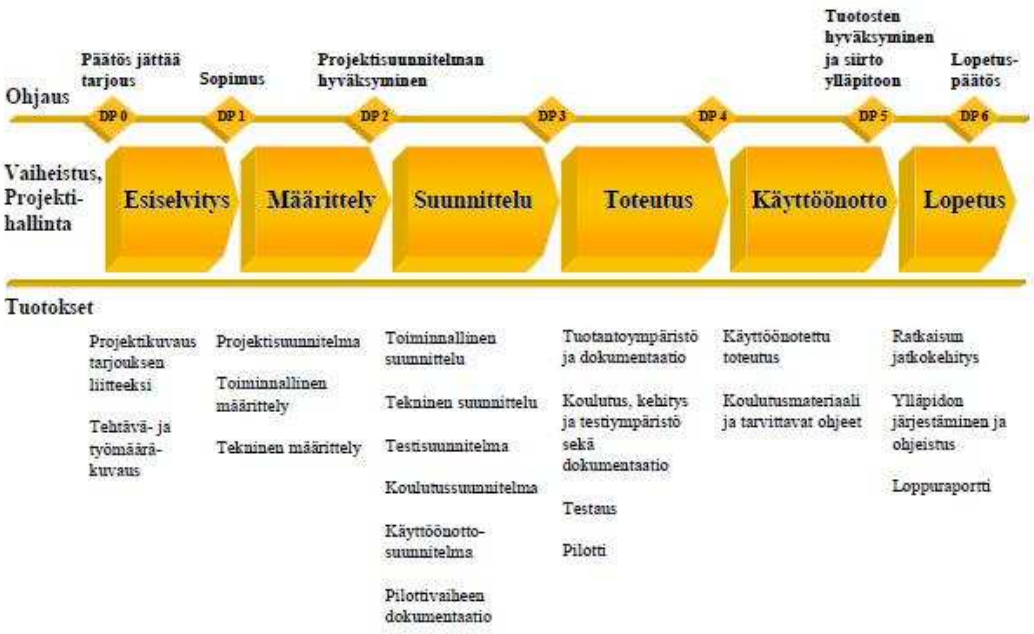
Kehitysprojektin malliksi valittiin soveltavin osin Cygaten asiakastoimituksissa sekä tuotekehityksessä käyttämä Cygaten sisäinen projektimalli. Projektimalli sekä projektin vaiheet on esitetty seuraavissa kappaleissa.

6.1 Projektimalli

Cygaten projektimalli perustuu kansainvälisten IPMA -organisaation (International Project Management Association) sekä PMI -organisaation luomiin projektin hallinnan käytäntöihin. Cygaten projektimallia käytetään yrityksen tuottamissa ja johtamissa asiakastoimitus- sekä tuotekehitysprojekteissa. Projektimallin tarkoituksena on selkeiden vaiheiden ja johtamisen avulla varmistaa seuraavat asiat:

- Projektille asetetut tavoitteet saavutetaan.
- Projektin laatu ja mahdollinen asiakastyytyväisyys on varmistettu.
- Vastuut on kommunikoitu selkeästi sekä eri projektiosapuolien välillä on yhteisesti sovitut toimintatavat.
- Projektin vaiheista raportoidaan ja tiedotetaan säännöllisesti.
- Projektissa syntyvä osaaminen ja kokemusperäinen tieto on hallittua.
- Vakioitujen toimintamallien kautta taataan varmuus ratkaisun tai kehityksen toteuttamiseen.

Cygaten projektimallin vaiheet ja päätöksentekopisteet on esitetty kuviossa 5 esimerkinomaisesti asiakastoimitusten osalta:



Kuvio 5: Cygate projektimalli

Cygaten projektimallissa päätöksentekopisteiden vaatimukset ja eri vaiheet ovat tarkkaan määriteltyjä, ja jo tehtyjen ja hyväksyttyjen päätösten muuttaminen tietyn päätöksentekopisteen (DP) jälkeen ei projektissa enää onnistu.

Jokaisessa päätöksentekopisteessä päätetään jatketaanko projektia, lopetetaanko se, vai suunnataanko sitä jotenkin uudelleen.

DP pisteiden kuvaukset on esitetty alla:

DP0 - Projektiehdotuksen hyväksyminen ja esiselvityslupa

- Päätetään projektiesitysten ja -ehdotusten hyväksymisestä.
- Jos projektiehdotus hyväksytään, käynnistetään esiselvitysvaihe, joka määrittelee projektin tavoitteet, laajuuden, tuotokset, ehdot ja rajaukset asetusmäärittelydokumentilla sekä sen liitteillä.

DP1 - Esiselvityksen hyväksyminen ja suunnittelulupa

- Liiketoimintapäätös, jossa pohditaan projektin toteutettavuutta ja asetetaan budjetti suunnitteluvaiheelle DP2 -pisteeseen asti. Resurssit nimetään DP2 -pisteeseen asti.

- DP1-DP2:
    - järjestelmä, toiminnallisuus ja muut määrittelyt sekä alustava käyttötapaus on määritelty
    - alustava ratkaisuehdotus
    - tietoturva-analyysi
    - testaussuunnittelu
    - alihankkija- ja toimittajaneuvottelut.

DP2 - Projektisuunnitelman hyväksyminen ja toteutuslupa

- Liiketoimintapäätös, jolla vahvistetaan liiketoimintasuunnitelma, investoinnit, projektin budjetti sekä lopullinen projektiorganisaatio. Toteutusvaihe käynnistetään DP2 -hyväksynnällä. Mikäli esimerkiksi vaadittuja esitietoja ei ole saatu valmisteltua DP2 -kokoukseen mennessä, täytyy projektin asettajan tehdä päätös esimerkiksi projektin päättämisestä tai myöhästyttämisestä.
- DP2-DP3:
    - tekninen ja toiminnallinen määrittely
    - tietoturva-arkkitehtuurin analysointi.

DP3 - Lopullisen toteutussuunnitelman hyväksyminen ja etenemislupa

- Projektin lopullisen, yksityiskohtaisen suunnitelman hyväksyminen. Muutoksia ilman ohjattua muutostenhallintaa ei tämän jälkeen sallita.
- DP3-DP4:
    - tekninen toteutus
    - testaus
    - tuotantoon viennin valmisteleminen.

DP4 - Tuotosten hyväksyminen ja etenemislupa

- Hyväksytään projektin lopulliset tuotokset ja aloitetaan vastuiden siirron vaatimat toimenpiteet.
- DP4-DP5:
  - testauksen loppuun suorittaminen
  - tuotantoon ja ylläpitoon siirron aloittaminen
  - pilotointi
  - tuotteen julkistamisen suunnittelu.

DP5 - Lopullisten tulosten hyväksyminen ja lopetustoimien aloituslupa

- Hyväksynnällä vahvistetaan, että projektin tuotokset vastaavat tavoitetta (riittävissä määrin), ja että vastuunsiirrot on asianmukaisesti suoritettu. Testitulokset evaluoidaan tässä DP -pisteessä.
- Annetaan lupa käynnistää projektin lopetustoimet.

DP6 - Projektin lopetuspäätös

- Vahvistetaan projektin päättäminen. Projektiorganisaatio on purettu, materiaalit ja laitteet on palautettu tai poistettu käytöstä, projekti- ja tuotedokumentaatiot on viimeistelty ja asianmukaisesti tallennettu, loppuraportti on esitetty projektin asettajalle ja projektin jatkoevaluoinnista vastaava henkilö on nimetty.
-

6.2 Projektin vaiheet

6.2.1 Esiselvitys ja projektisuunnitelma

Projektin esiselvitysvaiheen aikana tutustuttiin sekä yksityiskohtaisesti ISO/IEC 27001 -standardin vaatimuksiin että Cygaten nykyiseen dokumentaatioon. Lisäksi toimintatapojen ja prosessien osalta haastateltiin eri yksiköiden henkilöitä sekä ylintä johtoa nykyisten käytäntöjen kartoitusta varten. Haastattelumalliksi luotiin jo esiselvitysvaiheessa tulevia sisäisiä auditointeja tukeva toimintamalli,

jossa standardin eri osa-alueiden toimintaa tutkitaan vertaamalla luotua dokumentaatiota käytännön toimintatapoihin. Lisäksi esiselvitysvaiheen aikana valittiin sertifioijaksi Inspecta Sertifiointi Oy.

Esiselvitysvaiheen arviointi tehtiin peilaten haastatteluiden tuloksista saatuja tietoja sekä nykyisten dokumenttien sisältöä ISO/IEC 27001 -standardin valvonta- ja turvamekanismeihin sekä muihin vaatimuksiin. Esiselvityksen tuloksina havaittiin, että Cygaten nykyinen dokumentaatio tukee jo osittain ISO/IEC 27001 -standardin vaatimuksia. Suurimmat puutteet dokumentoinnissa kohdistuivat selkeiden roolien ja vastuiden määritykseen, sisäisten auditointien käytäntöihin, riskien hallinnan käytäntöihin, yleisiin tietoturvallisuusohjeistuksiin sekä liiketoiminnan jatkuvuussuunnittelun ja säännöllisten koulutusten dokumentointiin. Näiden havaintojen perusteella määriteltiin uudet luotavat dokumentit standardin vaatimusten täyttymiseksi.

Nykyinen dokumentaatio oli varsin kattavaa verrattuna standardin vaatimuksiin käyttöoikeuksien hallinnan, salassapitosopimusten, tietoturvapolitiikan sekä yleisen tietoturvallisuuden hallinnan osalta. Kuitenkin jo olemassa olevien dokumenttien osalta tarvittiin päivityksiä ja tarkennuksia. Havaintojen perusteella päätettiin muokata näitä jo luotuja dokumentteja standardin vaatimusten täyttymiseksi.

Haastatteluiden tuloksista toisaalta pystyttiin huomaamaan joistain osa-alueista, että toiminta esimerkiksi järjestelmien tietoturvallisuuden takaamiseksi ja valvomiseksi on jo olemassa, mutta sitä ei ole dokumentoitu. Esimerkiksi tietoturvapäivityksiä järjestelmiin tehtiin säännöllisesti, johtoryhmä arvioi riskejä jatkuvana prosessina sekä poikkeustilanteisiin oli varauduttu, mutta selkeä dokumentaatio näiltä osa-alueilta puuttui.

Lisäksi esiselvitysvaiheen aikana määriteltiin tietoturvallisuuden hallintajärjestelmän kattavuus. Kattavuus määriteltiin seuraavasti: ”Cygaten palvelutuotannon tietoturvallisuuden hallintajärjestelmä, kattaen palvelun kehitys-, tuotanto- ja asiakaspalveluprosessit”. Kattavuusmäärittely perustui asiakkaiden vaatimuksiin jatkuvien palveluiden tietoturvallisuuden osalta sekä toisaalta ylimmän johdon määrittelemän strategiaan, jossa Cygaten jatkuvat palvelut muodostavat Cygaten tulevaisuuden kannalta liiketoimintojen kannattavan kasvun. Kattavuusmäärittelyn avulla muodostuivat standardin suojattavien kohteiden määrittely osaksi soveltamissuunnitelmaa. Toisaalta kattavuusmäärittelyn avulla soveltamissuunnitelmasta pystyttiin rajaamaan pois standardin vaatimat turvamekanismit, jotka eivät tule koskemaan Cygaten käytettävyyspalveluita. Pois rajattaviksi turvamekanismeiksi muodostui esimerkiksi ulkoistettu ohjelmistokehitys sekä verkossa tapahtuvaan liiketoimintaan liittyvät turvamekanismit, joita Cygaten palvelutuotannossa ei ole käytössä. Myös projektin alustava aikataulu ja kustannukset käytiin läpi.

Esiselvitysvaiheen aikana muodostettiin myös projektin aikaista ohjausta varten Cygaten projektimallin mukainen ohjausryhmä. Koska projekti liittyi oleellisesti Cygaten strategiaan, ohjausryhmän jäsenet koostuivat johtoryhmän jäsenistä, ja ohjausryhmän toimintaa johti toimitusjohtaja. Tällä toiminnalla pystyttiin varmistamaan projektille riittävä tuki, ja reagoimaan mahdollisiin haasteisiin riittävän tehokkaasti ja nopeasti. Projektipäällikön vastuuksi määriteltiin raportoida viikoittain ohjausryhmälle projektin eri vaiheiden etenemisestä sekä mahdollisista aikatauluun, kustannuksiin tai resursseihin kohdistuvista uhkista. Lisäksi projekti otettiin seurantaan jatkuvana prosessina osana Cygaten johtoryhmän työskentelyä.

Projektin resursseiksi määriteltiin kattavasti henkilöitä eri yksiköistä, jotta pystyttiin varmistamaan riittävä sitoutuminen organisaation eri osista. Projektiorganisaatio muodostui henkilöstöhallinnon edustajista, tietojärjestelmien omistajista, prosessien omistajista sekä Cygaten tietoturvallisuudesta vastaavista henkilöistä. Lisäksi laatupäällikkö osallistui projektin työskentelyyn, koska hänen vastuul-

laan tulisi olemaan standardin vaatima jatkuvan parantamisen tuotosten seuraamien sekä sisäisten auditointien toteutus.

Esiselvitysvaiheen jälkeen hyväksytettiin projektin ohjausryhmällä projektin aikataulu, laajuus, resurssit sekä sertifioija, joista muodostui kustannusten osalta projektin suunnitelma. Projektisuunnitelman hyväksynnän yhteydessä käynnistettiin myös Inspectan kanssa standardin sertifiointiprosessiin liittyvät toimenpiteet, ja tehtiin sertifiointihakemus. Inspectan kanssa pidetyssä suunnittelukokouksessa vahvistettiin yhdessä dokumentaation nykytila sekä suunniteltiin tarkempi aikataulu.

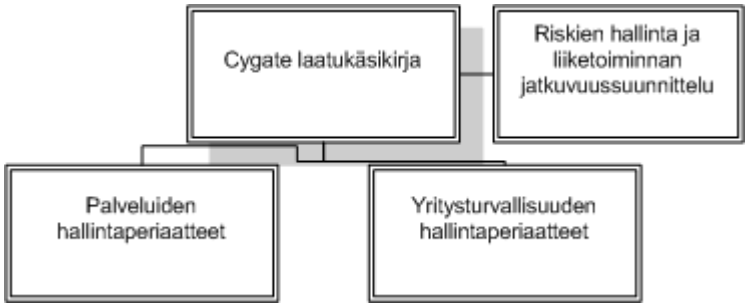
6.2.2 Projektin toteutus

Projektin varsinainen toteutus suoritettiin jakamalla tehtävät projektin resursseille peilaten sitä ISO/IEC 27001 -standardin liitteen A turvamekanismien vaatimuksiin, koska tämän toiminnan avulla voitiin varmistua kaikkien turvamekanismien täyttyminen standardin vaatimusten ja kohdemäärittelyn mukaisesti. Turvamekanismeja käytettiin eräänlaisena tarkistuslistana projektin seurannassa. Turvamekanismien listasta rakennettiin lisäksi soveltamissuunnitelma tietoturvallisuuden hallintajärjestelmälle, joka on pakollinen osa-alue ISO/IEC 27001 -standardissa.

Toteutuksessa huomioitiin rinnakkain käynnissä olevan ISO/IEC 20000 standardin käyttöönoton vaatimukset. Tämän johdosta hallintajärjestelmät päätettiin yhdistää yhdeksi laajemmaksi hallintajärjestelmäksi yhteneviltä osin standardien vaatimusten mukaisesti sekä toisaalta päällekkäisten tehtävien tekemisen välttämiseksi. Hallintajärjestelmän laadinnassa huomioitiin myös mahdolliset myöhemmin luotavat hallintajärjestelmät kuten ISO 9001 ja ISO 14001, joiden käyttöönotosta tulevaisuudessa Cygaten johto oli jo tehnyt alustavan päätöksen. Yhteisiksi osioiksi eri standardien vaatimuksista valittiin muun muassa seuraavat asiat:

- johdon vastuu
- johdon katselmoinnit
- sisäisten auditointien käytännöt
- jatkuvan parantamisen toimintamallit
- riskien hallinta- ja liiketoiminnan jatkuvuussuunnittelu
- asiakirjojen ja tallenteiden ohjaus.

Nämä edellä mainitut osa-alueet kuvattiin projektin aikana Cygaten laatukäsikirjassa, joka toimii Cygaten hallintajärjestelmien päädokumenttina. Tällä rakenteella pystyttiin turvaamaan ja varmistamaan tulevien ISO 9001 ja ISO 14001 -standardien liittäminen osaksi laajempaa laadun hallintajärjestelmää. Dokumentaation rakenteeksi muodostui alla olevan kuvion 6 mukainen rakenne:



Kuvio 6: Cygaten hallintajärjestelmien rakenne

Cygaten laatukäsikirjan sisällöksi muodostuivat yleiset laadun hallintaperiaatteet ja -tavoitteet, organisaation kuvaus, yrityksen prosessit, roolit ja vastuut, osaamisen hallinta ja koulutus, johdon vastuiden ja katselmointien kuvaus, sisäisten auditointien käytännöt sekä jatkuvan parantamisen käytännöt, joita voidaan pitää myös muiden hallintajärjestelmien osalta yhteisinä osa-alueina. Näiden kuvausten avulla saavutettiin edellä mainittujen osa-alueiden kuvaaminen ISO/IEC 27001 -standardin mukaisesti.

Riskien hallinta ja liiketoiminnan jatkuvuussuunnittelu -dokumentissa kuvattiin liiketoiminnan jatkuvuuteen liittyvät käytännöt sekä riskien arviointiin liittyvät

käytännöt ja hyväksymistavat. Riskien hallinnan ja tietoturvallisuuden hallintajärjestelmän soveltamisen osalta dokumentin liitteeksi muodostui ISO/IEC 27001 -standardin soveltamissuunnitelma, koska ISO/IEC 27001 -standardissa riskit, suojattavat kohteet, turvamekanismit ja mittarit on hyvä sitoa yhdeksi kokonaisuudeksi. Soveltamissuunnitelma kuvaa Cygaten riskit, suojattavat kohteet, mittarit sekä käytettävät turvamekanismit linkitettyinä toisiinsa standardin vaatimusten mukaisesti.

Soveltamissuunnitelman sisältö on kuvattu liitteen 1 sivuilla 1–22 sisältäen riskien hallinnan toimenpiteet, suojattavat kohteet, mittarit sekä käytössä olevat turvamekanismit, jotka ovat Cygaten luottamuksellista liiketoimintatietoa. Riskien hallinnan seuranta- ja arviointitaulukko on kuvattu liitteen 1 sivulla 23 , ja suojattavien kohteiden määrittelytaulukko liitteen 1 sivulla 24. Liite 1 on luokiteltu salaiseksi.

Riskien luokittelun osalta päätettiin noudattaa kuvion 7 esittämää tapaa, jonka avulla jokaiselle riskille luotiin riskiluokitus sen todennäköisyyttä ja vaikutusta arvioiden, jotta kunkin riskin osalta saatiin kokonaiskäsitys sen vaikutuksesta Cygaten liiketoiminnalle. Riskit luokiteltiin lisäksi osana soveltamissuunnitelmaa, ja luonnollisesti jokaiselle riskialueelle sekä riskille muodostettiin selkeät omistajat, jotta voitiin varmistua riskien asianmukaisesta käsittelystä sekä niiden kontrolloinnista. Riskien hallinnan osa-alueiksi muodostuivat standardin kattavuusmäärittelyn mukaisesti talouteen, henkilöstöön, tietojärjestelmiin, prosesseihin, teknologioihin, lakiasioihin sekä prosesseihin liittyvät riskit.

	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost certain (5)	Low	Medium	Medium	High	High
Likely (4)	Low	Medium	Medium	High	High
Moderate (3)	Low	Low	Medium	Medium	High
Unlikely (2)	Low	Low	Low	Medium	Medium
Rare (1)	Low	Low	Low	Low	Low

Kuvio 7: Riskien luokitus

Laatukäsikirjan liitteeksi muodostettiin yritysturvallisuuden hallintaperiaatteet -dokumentti, joka kuvaa yleisellä tasolla tietoturvallisuuden vastuut sekä pääsy- ja käyttöoikeuksien hallinnan, tietojen ja järjestelmien suojauksen, tietojärjestelmien ja palveluiden, tietoliikenteen, projektityön, fyysisen turvallisuuden, ulkoistamisen ja alihankinnan tietoturvaperiaatteet standardin mukaisesti. Lisäksi dokumentti kuvaa tietoturvallisuuden tavoitteet sekä yleisellä tasolla raportoinnin, tarkastuksen ja valvonnan, rikkomusten ja laiminlyöntien sekä poikkeuksien hallinnan periaatteet.

Yritysturvallisuuden hallintaperiaatteiden yleisiä määrityksiä täydennettiin kuvaamalla eri osa-alueita tarkemmin erillisissä dokumenteissa, jotta pystyttiin varmistamaan standardin vaatimusten riittävä kattavuus. Dokumentit muodostuivat seuraavista politiikoista, sopimuksista, ohjeista ja kuvauksista:

- yritysturvallisuuspolitiikka
- tietojen suojaus, luokittelu ja käsittely
- pelastussuunnitelma
- käyttöoikeuksien ja pääsyn hallinnan prosessi
- sitoumus yritysturvallisuuden noudattamisesta rooleineen ja vastuineen
- salassapitosopimukset henkilökunnalle, sidosryhmille sekä sidosryhmien henkilökunnalle
- toimenpidelistat uusille ja lähteville henkilöille sekä henkilön tehtävien muuttuessa
- tietoturvallisuusohjeistus käyttäjille sekä ylläpitäjille
- turvallisuuskuvaukset suojattavista kohteista
- tietoturvallisuuden koulutusmateriaali.

Henkilökunnalle tietoturvallisuuden hallintajärjestelmän vaatimukset kuvattiin selkiytetyssä muodossa yritysturvallisuuspolitiikka dokumentissa sekä osana rooleja ja vastuita. Tällä toiminnalla pystyttiin varmistamaan henkilökunnan tietoisuus tietoturvallisuuden vaatimuksista esittämättä asioita turhan yksityiskohtaisesti.

6.2.3 Käyttöönottovaihe

Käyttöönottovaiheessa projektin toteutusvaiheessa luodut dokumentit, toimintatavat sekä ohjeistukset hyväksytettiin johdolla sekä projektin ohjausryhmällä, ja ne julkaistiin koko Cygaten henkilökunnan käyttöön. Lisäksi luodun dokumentaation ja toimintatapojen käyttö varmistettiin kouluttamalla koko henkilökunta, ja sitoutuminen tietoturvallisuuden noudattamiseen varmistettiin kirjallisen sitoumuksen muodossa.

Käyttöönottovaiheessa asianmukainen jalkautus kaiken kaikkiaan Cygaten organisaatioon toteutettiin noudattaen oleellisia muutosjohtamisen periaatteita sekä Cygaten muutoshallintaprosessia, jotta voitiin varmistua standardin periaatteiden noudattaminen. Henkilökunnan sitoutuminen varmistettiin projektin aikaisella tehostetulla viestinnällä eri vaiheiden edetessä. Viestinnän avulla valmisteltiin henkilökunta muutoksiin. Lisäksi toimintatapojen muutokset koulutettiin osana Cygaten henkilöstötilaisuuksia, joissa esitettiin tarvittavat muutokset henkilökunnalle perustellen. Koulutuksista muodostui lisäksi jatkuva toimintatapa, jonka avulla tietoisuus tietoturvallisuudesta pystyttiin varmistamaan. Tänä päivänä aina osana Cygaten henkilöstötilaisuuksia käydään läpi tietoturvallisuuden tilannekatsaus sekä mahdollisia koulutuksia tietoturvatietoisuuden parantamiseksi.

Käyttöönottovaiheessa esimiehille painotettiin ylimmän johdon toimesta toimintatapojen muutosten tärkeyttä, ja lisäksi ylimmän johdon ja esimiesten esimerkillisen käyttäytymisen avulla varmistettiin toimintatapojen jalkautus. Lisäksi

osaksi esimiestyöskentelyä määriteltiin tietoturvatietoisuuden korostaminen ryhmätapaamisten yhteydessä. Projektin aikana ja toisaalta jo ennen projektia, projektin lähtökohdista viestittiin ylimmän johdon ja projektipäällikön toimesta, jotka omalta osaltaan varmistivat henkilökunnan sitoutumisen projektiin.

Olennaisena osana käyttöönottovaihetta oli, että standardin vaatima jatkuvan parantamisen prosessi käynnistettiin, sekä tietoturvallisuuden valvonta ja seuranta aloitettiin. Käytännössä jatkuvan parantamisen prosessi tarkoitti laatupäällikön johtamia sisäisiä auditointeja standardin kattavuuden mukaisille suojattaville kohteille, riskien hallinnan arviointeja sekä johdon katselmuksia. Sisäisten auditointien tuloksista muodostettiin vastuumäärittelyineen tehtävät korjaavien toimenpiteiden listalle jatkuvan parantamisen toteutumisen takaamiseksi.

Standardin vaatimien periaatteiden ja toimintatapojen toteutumisen arviointi käynnistettiin lisäksi aloittamalla suojattavien kohteiden tietoturvallisuuden ja luotujen toimintatapojen mittaaminen. Mittarit luotiin riittävän yksinkertaisiksi ja selkeiksi, sillä aiempien projektien käytännön kokemusten kautta oli opittu, että mittareiden tulee olla helppoja toteuttaa, sekä toisaalta mittareita ei tule olla liian paljoa.

Osana käyttöönottovaihetta projektin tulokset, eli tuotetut dokumentit, käytiin läpi standardin sertifiointiprosessin ennakkoarvioinnin kautta yhdessä Inspectan kanssa. Tämän toiminnan avulla pystyttiin varmistumaan vielä ulkoisen arvioijan toimesta standardin vaatimusten täyttymisestä.

6.2.4 Projektin lopetus

Projektin lopetusvaiheessa ohjausryhmällä hyväksytettiin projektin kokonaistuotokset, eli dokumentit, toimintatavat sekä ennakkoarvioinnista saatu palaute. Ennakkoarvioinnin palautteesta pystyttiin tulkitsemaan, että luodut dokumentit

sekä toimintatavat tukevat ISO/IEC 27001 -standardin sertifiointia. Lopetusvaiheen yhteydessä lisäksi määriteltiin aikataulu varsinaiselle sertifiointiarvioinnille sekä suoritettiin johdon katselmus. Projektin lopetuksesta voidaan todeta, että projektin tavoitteet saavutettiin, eli valmius Cygatelle edetä varsinaiseen sertifiointiarviointiin oli toteutunut.

7 POHDINTA JA JATKOTOIMENPITEET

Kansainvälinen ISO/IEC 27001 -standardi tarjoaa organisaatioille kattavat menetelmät tietoturvallisuuden hallintaan riippumatta organisaation luonteesta tai tyypistä. Voidaan siis yleisesti todeta, että ISO/IEC 27001 -standardin avulla kaiken tyyppiset organisaatiot voivat varmistaa tietoturvallisuuden hallittavuuden sekä toteutumisen kaikkien sidosryhmien välisessä toiminnassa sekä tietojen vaihdossa. Standardi takaa silloin, kun esimerkiksi palveluntarjoajat ovat kyseessä, että heidän asiakkaillaan on luottamus palveluntarjoajan tietoturvallisuudesta. Tämä oli lähtökohtana myös Cygate Oy:n valmistautumiselle ISO/IEC 27001 -standardin sertifiointiin.

ISO/IEC 27001 -standardi on todella kattava tietoturvallisuuden hallintaan liittyvä standardi, ja se vaatii organisaatiolta sitoutumista sekä jatkuvaa panostusta tietoturvallisuuden hallintaan. Standardin käyttöönotto voi olla laaja ja raskas projekti, mikäli organisaation perusasiat tietoturvallisuuden osalta eivät ole kunnossa. Käyttöönotto kannattaa tehdä suunnitelmallisen projektin kautta, jotta voidaan varmistaa selkeä aikataulu, kustannukset, resurssit sekä arvioida kattavasti projektin tuotokset. Mikäli organisaatiolla ei ole mahdollisuutta tutustua riittävän kattavasti standardin vaatimuksiin, on syytä harkita organisaation ulkopuolisen konsultin käyttöä apuna. Kaiken kaikkiaan voidaan todeta, että standardin käyttöönotolle tulee varata riittävästi aikaa, jotta voidaan osoittaa dokumentaation lisäksi toimintatapojen toteutuminen sekä toisaalta sisäisten auditointien, riskien hallinnan ja jatkuvan parantamisen tehtävien toteutuminen organisaatiossa.

Standardi takaa organisaatiolle selkeät tavat, toimintaohjeet sekä määritelmät tietoturvallisuuden toteuttamiseksi ja valvomiseksi. Olennaista standardin käyttöönoton yhteydessä on määritellä ja rajata selkeästi standardin kohde, ja soveltaa standardia kohdemäärittelyn mukaisesti. Standardin vaatimukset tarjoavat soveltamismahdollisuuden, ja toisaalta tiettyjen osa-alueiden pois rajaaminen on mahdollista perustellen. Kohdemäärittelyn avulla pystytään varmistumaan selkeän ja yksinkertaisen kokonaisuuden muodostamisesta.

Toisaalta monissa organisaatiossa standardin käyttöönotto vaatii paljon muutoksia toimintatapojen suhteen. Käyttöönottovaiheessa on hyvä varmistaa jatkuvalla viestinnällä sekä tavoitteiden perustelulla organisaation henkilökunnan sitoutuminen tietoturvallisuuden hallintaperiaatteiden noudattamiseksi sekä muutosvastarinnan välttämiseksi. Myös henkilökuntaa tulee ottaa mukaan mahdollisimman laajasti eri prosessien osa-alueilta kehittämään omaa toimintaa, jotta voidaan varmistua standardien vaatimusten toteutuminen.

Cygate Oy:n tapauksessa lähtötilanne standardin käyttöönottamiseksi oli hyvä, sillä yritys on jo vuosien ajan panostanut systemaattisesti tietoturvallisuuden hallintaan, ja toisaalta tarjoaa ratkaisuja asiakkailleen tietoturvan hoitamiseksi. Lisäksi yrityksen osalta ei tarvinnut tehdä mittavia muutoksia esimerkiksi teknisiin ratkaisuihin tai toteutuksiin, sillä ne täyttivät ja tukivat pääsääntöisesti suoraan standardin vaatimuksia.

Cygaten käyttämä järjestelmällinen projektimalli tuki lisäksi loistavasti standardin käyttöönottoa. Lisäksi muutosjohtamisen periaatteet varmistivat hyvin standardin käyttöönoton yrityksessä. Eri organisaation osista koostunut projektiryhmä takasi laaja-alaisesti tietoisuuden vaatimuksista, sekä esimiesten sitouttaminen johdon toimesta omalta osaltaan varmisti eri ryhmien toimintojen muutokset. Projektin aikaisella viestinnällä pystyttiin myös varmistamaan henkilökunnan tietoisuus sekä perustelemaan tarvittavien muutosten vaikutukset muutosvastarinnan välttämiseksi.

Cygate Oy:n osalta voidaan todeta, että kehitysprojektin aikana saavutettiin projektille asetetut tavoitteet, eli valmiudet standardin sertifiointiarviointiin. Valmius standardin vaatimuksiin varmistettiin yhdessä valitun sertifioijan Inspecta Sertifiointi Oy:n kanssa lisäksi ennakkoarvioinnin kautta. Tietenkin ennakkoarvioinnin tulokset osoittavat, että työtä sertifiointiin valmistautumiseksi täytyy jatkaa, koska kyseessä on vielä vasta äskettäin luotu kokonaisuus tietoturvallisuuden hallintaan. Sertifiointiarvioinnin yhteydessä organisaation tulee osoittaa luodun hallintajärjestelmän toiminta todisteiden valossa, ja luonnollisesti näitä ei Cygaten tapauksessa voi vielä olla kattavasti.

Jatkotoimenpiteinä Cygate Oy:n osalta voidaan todeta, että yrityksen tulee jatkaa luodun tietoturvallisuuden hallintajärjestelmän kehittämistä standardin vaatiman prosessinomaisen toiminnan kautta. Tämän avulla yritys saa osoitettua varsinaista sertifiointiarvioita varten riittävät todisteet hallintajärjestelmän käytöstä ja sen toiminnasta. Todisteita on hyvä olla usean kuukauden ajalta eri osa-alueilta. Cygaten valmistautumisprojektin päättyessä vuoden 2011 lopussa arvioidaan, että Cygatella olisi riittävät mahdollisuudet suorittaa varsinainen sertifiointi ISO/IEC 27001 -standardiin kevään 2012 aikana.

LÄHTEET

Allen, J. 2002. Verkkotietoturvan hallinta – CERT. Helsinki: Edita.

Humphreys, E. 2007. Implementing the ISO/IEC 27001 Information Security Management System Standard. Lontoo: Artech House.

Inspecta Sertifointi Oy. 2008. Tietoturvallisuusstandardi ISO 27001 -koulutus. Luentomateriaali.

Kuusela, H. & Ollikainen, R. 1999. Riskit ja riskien hallinta. Vammala: Vammalan kirjapaino.

Miettinen, J. 1999. Tietoturvallisuuden johtaminen. Jyväskylä: Gummerus.

Miettinen, J. 2002. Yritysturvallisuuden käsikirja. Jyväskylä: Gummerus.

Moisio, J. Tietoturvallisuuden hallintajärjestelmät, vaatimukset. http://www.ims.fi/sites/default/files/Tietoturvallisuuden_hallintajarjestelmat_vaatimukset.pdf. 8.12.2011.

Suomen standardisoimisliitto SFS. 2006. ISO/IEC 27001 – tietoturvallisuusstandardi liitteineen

Tietojärjestelmien tarkastus ja valvonta ry. 1997. Tietojärjestelmien tarkastuksen ja riskienhallinnan käsikirja. Jyväskylä: Gummerus.